

Security of Semi Device Independent QKD protocols against detector blinding attacks

Anubhav Chaturvedi,¹ Maharsi Ray,¹ Ryszard Veynar,^{2,*} and Marcin Pawłowski²

¹*Center for Computational Natural Sciences and Bioinformatics, IIIT-Hyderabad, Hyderabad-500032, India*
²*Institute for Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

While fully device-independent security in BB84-like one way QKD is impossible, it can be guaranteed against individual attacks in a semi device-independent scenario, where no assumptions on the characteristics of the hardware used are made except for the communication channel for which an upper bound on capacity is put. This approach is especially relevant in the context of recent *quantum hacking* attacks in which the eavesdroppers are able to remotely alter the behaviour of the devices used by the communicating parties. They are however unable to change the capacity of the channel. In this work we study the security of a semi device-independent QKD protocol against the detector blinding attacks. We find the critical detection efficiencies required for security for the eavesdroppers with and without quantum memory.

I. INTRODUCTION

In standard quantum key distribution (QKD) protocols the security proofs assume that the parties have access to the correct and exact specifications of the devices that they are using. This assumption is quite problematic. First of all it requires putting trust in the manufacturer of the devices, which may be not the best idea. The supplier can install backdoors, that enable him to compromise the security without being detected. Recently a lot of attention has been drawn to NSA which convinced RSA Security to set as a default in their products Dual_ECC_DRBG pseudorandom number generator which is considered to have such a backdoor[1]. Moreover, even if the manufacturer is honest, recent advances in *quantum hacking* [2] show that the adversary can remotely influence the behaviour of the devices during the protocol, effectively changing their characteristics. To cope with this issue the device independent (DI) approach has been introduced. There it was argued that if the parties violate Bell inequalities then, regardless of how their devices managed to do this, they can establish a secure communication. Although the term "DI" was first used in [3] the idea can be tracked back all the way to the original Ekert's paper [4]. Unfortunately, DI QKD is extremely hard to realize in practice and so far no experimental group has been able to do this. The main reason for this is so-called detection efficiency loophole [5], which states that if the probability of registering a particle by the detectors used in the experiment is below a certain (usually very high) value then the results of the experiment are inconclusive, in other words: local, realistic description of its results cannot be ruled out. Ruling out this description is a necessary, although not always sufficient, condition for DI security. Another problem faced in this scenario is that it can be applied only to protocols based on entanglement which are much more complicated than prepare-and-measure ones like BB84 [6].

These two issues are addressed in the semi-device in-

dependent (SDI) approach [7]. There a prepare-and-measure scenario is considered and again no assumptions are made on the inner working of the devices used. Prefix "semi" is warranted by the fact that an upper bound on the capacity of the communication channel is made. Assuming this bound is well justified for both honest and dishonest manufacturer. In latter case the parties can study the devices delivered and, while it is almost impossible to fully characterize them, it is much easier to establish the effective dimension of the Hilbert space in which the states are being prepared. When the supplier is honest but the protocol is subject to a quantum hacking attack, the limitations on the technology available to the eavesdropper make increasing the channel capacity extremely difficult. In fact, to our knowledge, all the quantum hacking attacks published so far did not increase this capacity. Also, because only one side employs the detectors, the requirements on their efficiency are lower than in the DI case.

Another relaxation of the DI paradigm is measurement-device independent (MDI) scenario [8][13]. There three devices are used. Two communicating parties, with perfectly characterized hardware are sending the particles to the third one which makes the measurements. We do not make any assumptions on the properties of the third device. The difference between MDI and SDI scenarios is that the former one is more complicated (ie. requires more devices and more sophisticated measurements) and does not allow for any changes in the preparation devices (which is a big disadvantage because even small changes can lead to the loss of security [10]). On the other hand, it was shown [8] that MDI scenario thwarts quantum hacking attacks for any efficiency of the detectors.

The aim of this paper is to establish the critical detection efficiencies for the SDI case. We start by defining the classes of attacks against which we want to be secure. We consider individual attacks in which eavesdropper has or does not have access to quantum memory. Then we take the most well-known SDI QKD protocol [7] and calculate the detection efficiencies required in both cases. Next we propose a modification of this protocol which

* savitarveynar@web.de

substantially reduces these requirements.

II. DEVICE CONTROLLING ATTACKS

In papers [2, 16] authors gave a simple description of the blinding attacks based on detection efficiency loop-hole. They also experimentally showed that the idea can be successfully implemented for various protocols. Assume that Eve has perfect detectors while Bob's have 50% efficiency. Eve intercepts the signal sent from Alice to Bob who are communicating via BB84 setup and measures it. After that Eve encodes her detection results into specially tailored bright pulse of light and resends it to Bob. Because of physical properties of the signal and his detectors Bob will only have a detection result if his measurement is in the same basis as Eve's. It means that detectors used by Bob will work with 100% efficiency if Eve's and Bob's settings are the same and will not work at all in the other case. On average detectors will work with 50% efficiency which does not cause any suspicions. After the raw key exchange, Bob and Eve have identical bit values and basis choices which after sifting, error correction and privacy amplification made by classical communication allows her to get the identical final key. This is how Eve, by active control of a detector used by Bob can secretly learn exchanged key. More about that type of control can be found in [15].

In [10] a different approach is presented. Here Eve apart from exploiting her possibility of interfering during the calibration of Alice's device introduces a slight modification in it.

These examples show the need for more general security conditions where Eve is quite powerful and can influence all the devices used in the protocol. However there are natural limits to what she can do. Her modifications should not be significant in order to avoid detection, e.g. she cannot make the device use additional degree of freedom of the communicated system to encode more information as this would require introducing a lot of new elements into the device. This justifies taking the SDI approach in which we assume that the eavesdropper can change the characteristics of the devices used but cannot increase the dimension of the system sent by Alice.

III. SDI SECURITY AND ASSUMPTIONS

DI QKD protocol bases its security on violation of some Bell inequality [11] associated with the scenario. Key rate, in this case, can be maximized by reaching the quantum bound of this inequality. On the other hand, SDI is a prepare and measure key distribution protocol with the fixed dimension of the communicated system between Alice and Bob [7]. To be more precise this limitation is just for dimension of the signal emitted by Alice and doesn't hold for what Bob is receiving. This is the most advantageous case for Eve, which furthermore

reflects the fact that in blinding attacks the pulse sent by her to Bob's lab carries substantially more than one bit of information.

SDI QKD scheme bases its security on beating the classical bound on efficiency of a related communication complexity task. In [7] the task used was a $2 \rightarrow 1$ Quantum Random Access Code (QRAC)[12]. In it Alice encodes her two input bits $a_0, a_1 \in \{0, 1\}^2$ into a qubit ρ_{a_0, a_1} . Bob gets only one input bit $b \in \{0, 1\}$ and chooses his projective measurements M_b^B based on it. His task is to return $B = a_b$ with as high average probability as possible. In the QKD protocol after many subsequent rounds of the QRAC Bob announces his choice of b for each round. The a_b is kept secret and as the bit of key for that round.

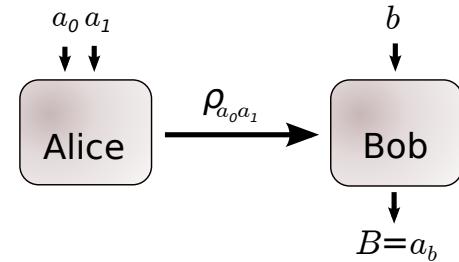


FIG. 1. SDI protocol based on $2 \rightarrow 1$ QRAC without Eve.

Probability for Bob to obtain (for fixed settings a_0, a_1 and b) the result i is $P(B = i | a_0, a_1, b) = \text{tr}(M_b^{B=i} \rho_{a_0, a_1})$ for $i \in \{0, 1\}$. Here, $M_b^{B=i}$ are projection operators such that $\sum_{i \in \{0, 1\}} M_b^{B=i} = \mathbf{I}$. The security parameter in this case is an average success probability for $2 \rightarrow 1$ QRAC. It is given by

$$P_B = \frac{1}{8} \sum_{a_0, a_1, b \in \{0, 1\}^3} P(B = a_b | a_0, a_1, b). \quad (1)$$

Alice and Bob can now establish a secret key by keeping a_b after Bob reveals his choice b for each round. The key rate can be as high as $I(A : B) = 1 - H(P_b)$ if Eve does not interfere.

IV. ANALYSIS OF THE ATTACKS

We make the following assumptions about the attacks of Eve:

1. She cannot influence the dimension of the system leaving Alice's lab
2. She performs individual attacks
3. For each bit of the key the whole information she has about it is stored in a bit representing her best guess of this bit (this models the situation in all proposals for blinding attacks)

4. Bob's and Alice's devices are controlled by Eve (she can make detectors work with 100% efficiency if she chooses to)

In this part of the paper we analyze two types of attacks on SDI protocol based on 2→1 QRAC.

1. Intercept/Resend (without quantum memory).
2. Delayed Measurement (with POVM and a qubit of quantum memory).

First attack due to its simplicity allows us to determine security conditions analytically. This is because we take Eve's measurements to be projective and she is the only one who sends information to Bob which makes it quite easy to parameterize (Fig.2). Later we extend the formalism and show that POVM measurements and quantum memory gives no advantage to Eve.

A. Intercept/Resend (IR)

Eve intercepts the signal transmitted from Alice to Bob and measures it according to her input $e \in \{0, 1\}$. This input is not absolutely necessary for our analysis but we introduce it to better model blinding attacks. It represents Eve's guess of what the input of Bob is going to be. It also allows us to be more general. In this work we assume "free will", i.e. that e and b are uncorrelated but in general it is possible to study models when this assumption is partially relaxed and measure Bob's "free will" by amount of correlations between e and b . Note that Eve being able to choose different detection probabilities for rounds when $e = b$ and $e \neq b$ artificially introduces correlations between e and b at the level of postselected rounds of experiment.

Eve uses the measurement M_e^E and obtains an output bit $E \in \{0, 1\}$. At this stage we can write Eve's probabilities of getting $E = i$ as

$$P(E = i|a_0, a_1, e, b) = P(E = i|a_0, a_1, e) = \text{Tr}(M_e^{E=i} \rho_{a_0, a_1}) \quad (2)$$

where the first equality is because of the fact that Eve gets her outcome E before Bob inputs b . Here, $M_e^{E=i}$ are projection operators such that $\sum_{i \in \{0, 1\}} M_e^{E=i} = \mathbf{I}$.

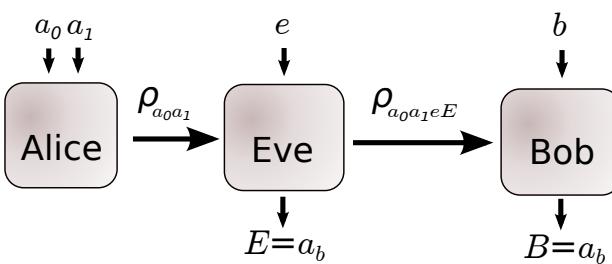


FIG. 2. IR attack implementation.

Eve then sends the state $\rho_{a_0, a_1, e, E=i} = M_e^{E=i}$ with probability $P(E = i|a_0, a_1, e)$ for $i \in \{0, 1\}$ as it represents her best knowledge about Alice's input.

According to assumption 4 Eve, for given η can design in advance all the states ρ_{a_0, a_1} and all measurements $M_{e,b}^B$ and M_e^E . However, in any given round of communication she is not aware of values of a_1 , a_2 and b having just e chosen by her.

Here, $M_{e,b}^{B=i}$ are projective operators satisfying $\sum_{i \in \{0, 1\}} M_{e,b}^{B=i} = \sum_{i \in \{0, 1\}} M_e^{E=i} = \mathbf{I}$. Bob's outcome probabilities are given by

$$P(B = i|a_0, a_1, e, b, E) = \text{Tr}(M_{e,b}^{B=i} \rho_{a_0, a_1, e, E}). \quad (3)$$

As Bob does not know Eve's output, we can obtain the probabilities by summing over the values of E which gives

$$\begin{aligned} P(B = i|a_0, a_1, e, b) &= \\ \sum_{j \in \{0, 1\}} P(E = j|a_0, a_1, e) P(B = i, E = j|a_0, a_1, e, b) &= \\ \sum_{j \in \{0, 1\}} \text{Tr}(M_e^{E=j} \rho_{a_0, a_1}) \text{Tr}(M_{e,b}^{B=i} M_e^{E=j} \rho_{a_0, a_1}). \end{aligned} \quad (4)$$

Success probabilities can be derived by taking an average over a_0 and a_1 and by the fact, that both, Bob and Eve are interested in finding value of a_b ($i = a_b$). We can write those probabilities in a simplified notation as

$$P_{E_b}^e = \frac{1}{4} \sum_{a_0, a_1} P(E = a_b|e, a_0, a_1) \quad (5)$$

$$P_{B_b}^{eb} = \frac{1}{4} \sum_{a_0, a_1} P(B = a_b|e, b, a_0, a_1). \quad (6)$$

Next we split Bob's detector efficiency $\eta_{avg} = P(\text{Click})$ into

$$\begin{aligned} \eta &= P(\text{Click}|e \neq b) \\ \eta_{e=b} &= P(\text{Click}|e = b). \end{aligned} \quad (7)$$

At this point Eve maximizes $\eta_{e=b}$ making it 1 as she wants Bob's device to return the outcomes as often as possible when she managed to guess his input. She also tries to minimize η . Only thing limiting her in doing so is the observed detection efficiency which can be easily verified by the users. $P(b) = P(b = e) = \frac{1}{2}$ since Eve has no control over Bob's settings. This leads to

$$\eta_{avg} = \frac{1 + \eta}{2}. \quad (8)$$

In this case observed success probabilities for Bob and Eve, postselected to rounds when Bob's detector registered a particle can be represented as weighted averages over inputs e and b

$$P_E(\eta) = \frac{1}{2(1 + \eta)} (P_{E_0}^0 + \eta P_{E_1}^0 + \eta P_{E_0}^1 + P_{E_1}^1). \quad (9)$$

$$P_B(\eta) = \frac{1}{2(1 + \eta)} (P_{B_0}^{00} + \eta P_{B_1}^{01} + \eta P_{B_0}^{10} + P_{B_1}^{11}) \quad (10)$$

Alice and Bob can establish a secret key if Shannon's mutual information between Alice and Bob is greater

than between Alice and Eve ($I(A : B) > I(A : E)$). Assumption 3 allows us to simplify this condition to

$$P_B(\eta) > P_E(\eta) \quad (11)$$

Therefore whenever $P_B(\eta)$ is higher than maximal success probability achievable by Eve $P_E^{\max}(\eta)$ protocol is secure. The optimization problem than boils down to finding

$$P_E^{\max}(\eta) = \max \left\{ \frac{P_{E_0}^0 + \eta P_{E_1}^0 + \eta P_{E_0}^1 + P_{E_1}^1}{2(1+\eta)} \right\} \quad (12)$$

with $P_{E_b}^e = \frac{1}{4} \sum_{a_0 a_1} \text{Tr}(\rho_{a_0 a_1} M_e^{E=a_b})$ and the maximization is taken over all possible measurements of Bob, Eve and preparations of Alice. Here we consider two cases:

1. Because of the fact that manipulations in Alice's lab are much more difficult for Eve than just taking control over Bob's lab by hijacking the signal, we start with an assumption that Eve cannot modify the encodings chosen by Alice. The states are fixed as

$$\begin{aligned} \rho_{00} &= |0\rangle\langle 0|, \\ \rho_{01} &= \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|), \\ \rho_{10} &= \frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|), \\ \rho_{11} &= |1\rangle\langle 1| \end{aligned} \quad (13)$$

which is an optimal set of states for the standard 2→1 QRAC. To find the maximum, projective measurements M_e^E has to be characterized by vectors from the same plane as the states (13). Then for $M_e^E = |M_e^E\rangle\langle M_e^E|$ we have

$$\begin{aligned} |M_e^{E=0}\rangle &= \cos \frac{\alpha_e}{2} |0\rangle + \sin \frac{\alpha_e}{2} |1\rangle \\ |M_e^{E=1}\rangle &= |M_e^{E=0}\rangle^\perp. \end{aligned} \quad (14)$$

This description allows us to simplify equation (12) to

$$P_E^{\max}(\eta) = \frac{1}{4} \left(2 + \cos \alpha_\eta + \frac{1-\eta}{1+\eta} \sin \alpha_\eta \right) \quad (15)$$

where $\alpha_\eta = \arctan \left(\frac{1-\eta}{1+\eta} \right)$ and $\eta \in [0, 1]$. By using (8) it can be easily transformed into $P_E^{\max}(\eta_{avg})$ which is a function of the observed detection efficiency. It is plotted in Fig.3.

2. In the second case a more powerful Eve fixes Alice's states to $\rho_{a_0, a_1} = |a_0, a_1\rangle\langle a_0, a_1|$. We parameterize them by

$$|a_0 a_1\rangle = \cos \frac{\alpha_{a_0 a_1}}{2} |0\rangle + e^{i\beta_{a_0 a_1}} \sin \frac{\alpha_{a_0 a_1}}{2} |1\rangle \quad (16)$$

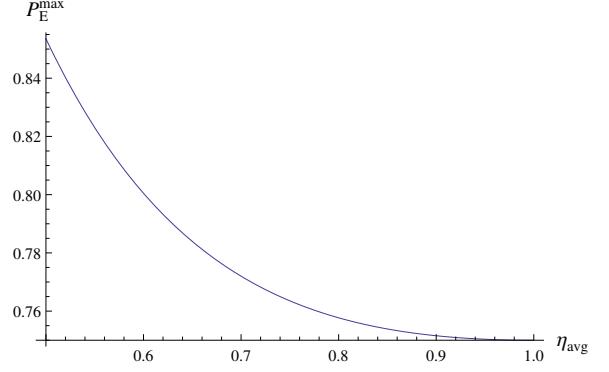


FIG. 3. Maximal success probability for Eve for SDI QKD based on 2 → 1 QRAC. Alice and Bob can verify security for any observed efficiency η_{avg} and Bob's success probability (P_B) against the maximum success probability of Eve ($P_E^{\max}(\eta_{avg})$).

where $\alpha_{a_0 a_1}$ and $\beta_{a_0 a_1}$ are chosen in advance by Eve. Plugging it, together with measurements

$$\begin{aligned} |M_e^{E=0}\rangle &= \cos \frac{\alpha_e}{2} |0\rangle + e^{i\beta_e} \sin \frac{\alpha_e}{2} |1\rangle \\ |M_e^{E=1}\rangle &= |M_e^{E=0}\rangle^\perp. \end{aligned} \quad (17)$$

into (12) we can define, for every $\eta \in (0, 1)$, a maximization problem over 12 independent variables. After performing numerical optimization we obtained the same results as our analytic calculations yield for the case without tampering with Alice's device (15).

These two cases show that controlling Alice's device in a protocol based 2→1 QRAC does not lead to any improvement for Eve.

B. Delayed Measurement (DM)

Now let us consider a more general approach where Eve is equipped with quantum memory of a single blank qubit ρ_{blank} (per signal). This description covers POVM measurements as well. After receiving the signal from Alice, Eve without any knowledge about Bob's selection of $b \in \{0, 1\}$ performs unitary transformation U_e on both qubits

$$\rho_{a_0, a_1, e} = U_e \rho_{a_0, a_1} \otimes \rho_{blank} U_e^\dagger \quad (18)$$

After this operation, she forwards to Bob the first subsystem keeping the second one. Eve does not receive any output at this point and delays the measurement on her particle until Bob publicly announces his setting b (Fig.4). Bob's projective measurement $M_{b,e}^B$ and Eve's measurement $M_{e,b}^E$ are designed by Eve to violate (11). The probabilities can be written as

$$P(E = i | a_0, a_1, e, b, B) = \text{Tr}((M_{e,b}^{E=i} \otimes M_{b,e}^B) \rho_{a_0, a_1, e}). \quad (19)$$

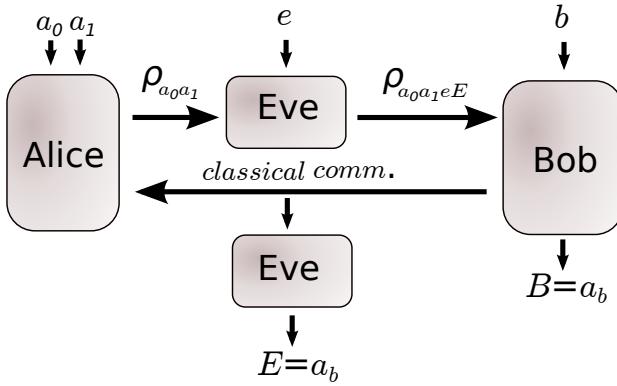


FIG. 4. DM attack implementation.

Because Eve does not know Bob's outcome, we can sum over the values of B and obtain

$$\begin{aligned} P(E = i|a_0, a_1, e, b) &= \sum_{B \in \{0, 1\}} \text{Tr}((M_{e,b}^{E=i} \otimes M_{e,b}^B) \rho_{a_0, a_1, e}) \\ &= \text{Tr}((M_{e,b}^{E=i} \otimes I)(\text{Tr}_B((I \otimes M_{e,b}^B) \rho_{a_0, a_1, e})). \end{aligned} \quad (20)$$

Bob's success probability can be expressed as

$$P(B = i|a_0, a_1, e, b) = \text{Tr}(M_{e,b}^{B=i} \text{Tr}_E(\rho_{a_0, a_1, e})). \quad (21)$$

To write formulas for observed probabilities we can use the same notations for Bob as before (6). Because of delayed measurement made by Eve we allow her probabilities (5) to depend on b . With this little extension and by taking $i = a_b$ we can define $P_E(\eta)$ and $P_B(\eta)$ in the same way as (9) and (10) respectively.

We have numerically optimized the guessing probability of Eve in this case and again obtained the same result as in the simplest case with IR attacks and no manipulation of Alice's device (Fig.3). We conclude that neither quantum memory with a more general measurement approach nor control over Alice's device does not give any advantage to Eve over controlling only the device of Bob. With the maximum quantum success probability $P_B \approx 0.85$ the security of this protocol against individual attacks of all the classes studied here is 50%. Now we modify the protocol to see if we can lower this number.

V. MODIFIED SDI PROTOCOL

Here we present SDI protocol based on 3→1 QRAC which is a straightforward generalization of the one from [7] and study its security against both types of attacks. In a 3→1 QRAC Alice is given three bits $a_0, a_1, a_2 \in \{0, 1\}^3$ depending on which she sends the state ρ_{a_0, a_1, a_2} , while Bob gets a classical trit, $b \in \{0, 1, 2\}$ and is required to guess the value of a_b . Bob's final output is $B \in \{0, 1\}$ and the success probability is labeled by $P_B = P(B = a_b)$. Eve wants to learn the bit a_b in order to establish the same key with Alice as Bob.

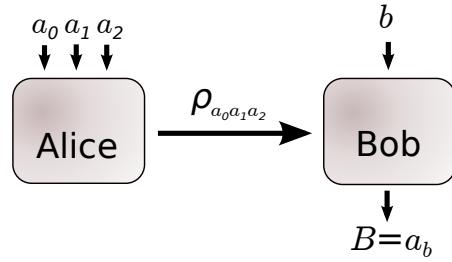


FIG. 5. SDI protocol based on 3→1 QRAC without Eve.

The whole structure, reasoning and notation (IR and DM) form SDI protocol based on 2→1 QRAC is kept. The average detection efficiency of Bob's detector is given by

$$\eta_{avg} = \frac{1 + 2\eta}{3}. \quad (22)$$

Eve's success probability, because of a larger number of settings is now

$$P_E(\eta) = \frac{1}{3(1 + 2\eta)} \left(P_{E_0}^0 + \eta(P_{E_1}^0 + P_{E_2}^0) + P_{E_1}^1 + \eta(P_{E_0}^1 + P_{E_2}^1) + P_{E_2}^2 + \eta(P_{E_1}^2 + P_{E_0}^2) \right). \quad (23)$$

where for IR $P_{E_b}^e = \frac{1}{8} \sum_{a_0 a_1 a_2} \text{Tr}(\rho_{a_0 a_1 a_2} M_e^{E=a_b})$. Analogous formulas can be written for $P_B(\eta)$. Here optimization problem can be solved by finding maximum $P_E^{max}(\eta)$ of (23) with $P_{E_b}^e = \frac{1}{8} \sum_{a_0 a_1 a_2} \text{Tr}(\rho_{a_0 a_1 a_2} M_e^{E=a_b})$. The maximization is carried over all states $\rho_{a_0 a_1 a_2}$ and measurements $M_e^{E=a_b}$. Again we can analyze two cases:

1. States emitted by Alice cannot be manipulated by Eve. Alice fixes them as

$$\begin{aligned} |000\rangle &= |0\rangle, \\ |001\rangle &= \frac{\sqrt{6}}{3}|0\rangle + \frac{\sqrt{3}}{3}|1\rangle, \\ |010\rangle &= \frac{\sqrt{6}}{3}|0\rangle + e^{i\frac{2\pi}{3}} \frac{\sqrt{3}}{3}|1\rangle, \\ |100\rangle &= \frac{\sqrt{6}}{3}|0\rangle + e^{-i\frac{2\pi}{3}} \frac{\sqrt{3}}{3}|1\rangle, \\ |111\rangle &= |000\rangle^\perp \\ |110\rangle &= |001\rangle^\perp \\ |101\rangle &= |010\rangle^\perp \\ |011\rangle &= |100\rangle^\perp \end{aligned} \quad (24)$$

where $\rho_{a_0 a_1 a_2} = |a_0 a_1 a_2\rangle \langle a_0 a_1 a_2|$. These states are an optimal encoding for the standard 3→1 QRAC. For measurements ($M_e^{E=a_b} = |M_e^{E=a_b}\rangle \langle M_e^{E=a_b}|$) we use general parametrization

$$\begin{aligned} |M_e^{E=0}\rangle &= \cos \frac{\alpha_e}{2}|0\rangle + e^{i\beta_e} \sin \frac{\alpha_e}{2}|1\rangle \\ |M_e^{E=1}\rangle &= |M_e^{E=0}\rangle^\perp. \end{aligned} \quad (25)$$

Encoding of Alice's states used here imposes symmetry by which the maximum value of $P_E(\eta)$ is given if $\beta_0 = \frac{\pi}{3}$, $\beta_1 = -\frac{\pi}{3}$ and $\beta_2 = \pi$. After substituting it to (23) we obtain

$$P_E^{max}(\eta) = \frac{1}{6} \left(3 + \cos \alpha_\eta + \frac{\sqrt{2}(1-\eta)}{1+2\eta} \sin \alpha_\eta \right) \quad (26)$$

where $\alpha_\eta = \arctan \left(\frac{\sqrt{2}(1-\eta)}{1+2\eta} \right)$. This is presented as a lower line of the plot Fig.6.

2. Analogously as before, we now assume that Eve can secretly change the way Alice's states are prepared. We start with simplified parametrization of Alice's encoding as

$$\begin{aligned} |000\rangle &= |0\rangle, \\ |001\rangle &= \cos \frac{\alpha}{2} |0\rangle + \sin \frac{\alpha}{2} |1\rangle, \\ |010\rangle &= \cos \frac{\alpha}{2} |0\rangle + e^{i\beta} \sin \frac{\alpha}{2} |1\rangle, \\ |100\rangle &= \cos \frac{\alpha}{2} |0\rangle + e^{-i\beta} \sin \frac{\alpha}{2} |1\rangle, \\ |111\rangle &= |000\rangle^\perp \\ |110\rangle &= |001\rangle^\perp \\ |101\rangle &= |010\rangle^\perp \\ |011\rangle &= |100\rangle^\perp \end{aligned} \quad (27)$$

where α and β are parameters controlled by Eve. In this case optimal encoding for standard 3→1 QRAC is reproduced for $\alpha = \arccos \frac{1}{3}$ and $\beta = 2\pi/3$.

After substituting it together with measurements (25) to (23) we maximize it over two parameters which leads to the solution. For $\eta \in \langle 0, \frac{3\sqrt{2}-4}{2} \rangle$ Eve's success probability is given by

$$\begin{aligned} P_E^{max}(\eta) &= \frac{1}{8} \left(4 + (1 + \cos \alpha_\eta) \cos \beta_\eta + \right. \\ &\quad \left. + \frac{2(1-\eta)}{1+2\eta} \sin \alpha_\eta \sin \beta_\eta \right) \end{aligned} \quad (28)$$

and for $\eta \in (\frac{3\sqrt{2}-4}{2}, 1)$ by a constant value

$$P_E^{max}(\eta) = \frac{3}{4}. \quad (29)$$

Here

$$\alpha_\eta = \arccos \left(\frac{1}{N(\eta)^2 - 1} \right) \quad (30)$$

$$\beta_\eta = \arctan \left(\frac{\tan(\alpha_\eta)}{N(\eta)} \right). \quad (31)$$

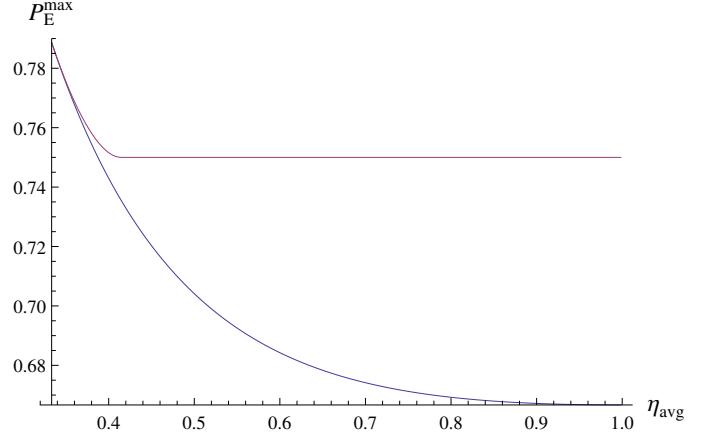


FIG. 6. Maximal success probability for Eve for SDI QKD based on 3→1 QRAC vs. η_{avg} (the upper line). Alice and Bob can verify security for any observed efficiency η_{avg} and (observed) Bob's success probability (P_B) against the maximum success probability of Eve ($P_E^{max}(\eta_{avg})$). The lower line describes maximal probability for Eve who cannot change the states ρ_{a_0, a_1, a_2} .

$$\text{where } N(\eta) = \frac{2(1-\eta)}{1+2\eta}.$$

After this we can move on to a more general description of $\rho_{a_0 a_1 a_2} = |a_0 a_1 a_2\rangle \langle a_0 a_1 a_2|$ where every vector $|a_0 a_1 a_2\rangle$ is parameterized as

$$\cos \frac{\alpha_{a_0 a_1 a_2}}{2} |0\rangle + e^{i\beta_{a_0 a_1 a_2}} \sin \frac{\alpha_{a_0 a_1 a_2}}{2} |1\rangle. \quad (32)$$

This increases the number of parameters controlled by Eve to 22. By numerical maximization we obtained the same limit as for the case with simplified parametrization (27) presented earlier. Here by tampering Alice's device Eve is able to visibly improve P_E^{max} (see Fig.6).

We have analyzed the case of DM attack against this protocol as well. We used analogous formulas to (20) and (21). By adapting previous algorithm to protocol based on 3→1 QRAC and running it over all parameters controlled by Eve we reconstructed lines presented in Fig.6. The security conditions for DM attack are again the same as for IR attack.

VI. CONCLUSIONS.

In this paper we analyzed individual *quantum hacking* attacks on SDI protocols based on QRACs where Eve can control all devices in use. Looking at these types of attacks was motivated by their recent experimental realizations. We have also shown that access to small quantum memory does not help the eavesdropper at all and conjecture that more memory does not change this state.

We analyzed two protocols. For SDI based on $2 \rightarrow 1$ QRAC Eve is not able to improve her situation by taking control over Alice's device which is quite surprising. Taking control only over the signal and Bob's detectors is the optimal attack for her and the critical detection efficiency, which depends on Bob's success probability, can be as low as 50%.

Changing SDI protocol into one based on $3 \rightarrow 1$ QRAC decreases the key rate but conditions for success probability are significantly lowered. Here the critical detector efficiency can be as low as 41.2% if Bob's success probability reaches quantum maximum. In this example one

can also see the advantage of manipulating Alice's device which was not the case for the previous protocol. Without this manipulation the critical detection efficiency is only 38.7%.

ACKNOWLEDGMENTS

This work is supported by the Foundation for Polish Science TEAM, ERC grant QOLAPS and NCN grant 2013/08/M/ST2/00626.

- [1] J. Menn, "Exclusive: Secret contract tied NSA and security industry pioneer", Reuters, December 20, 2013. Retrieved 25.03.2015.
- [2] B. Qi et al., Quantum Inf. Comput. **7**, 73 (2007); Y. Zhao et al., Phys. Rev. A **78**, 042333 (2008); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature photonics, **4** (10), 686-689 (2010); I. Gerhardt et al., Nature Commun. **2**, 349 (2011).
- [3] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501, (2007).
- [4] A. K. Ekert, Phys. Rev. Lett., **67**, 661 (1991).
- [5] P. Pearle, Phys. Rev. D, **2**, 1418, (1970).
- [6] C. Bennett and G. Brassard, Theoretical Computer Science, **560**, 7-11 (2014).
- [7] M. Pawłowski, N. Brunner, Phys. Rev. A **84**, 010302 (2011).
- [8] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
- [9] S. L. Braunstein, S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012)
- [10] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).
- [11] J. S. Bell, et al. Physics, 1.3: 195-200 (1964)
- [12] A. Ambainis and A. Nayak and A. Ta-Shma and U. Vazirani Journal of the ACM (JACM) **49.4** : 496-511 (2002)
- [13] S. L. Braunstein, S. Pirandola Phys. Rev. Lett. **108**, 130502 (2012)
- [14] V. Makarov and J. Skaar, Quant. Inf. Comp. **8**, 0622 (2008)
- [15] V. Makarov, New J. Phys. **11**, 065003 (2009).
- [16] Q. Liu, A. Lamas-Linares, C. Kurtsiefer, J. Skaar, V. Makarov, and I. Gerhardt, Rev. Sci. Instrum. **85**, 013108 (2014)